IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **11bk Spec text for NDP Announcement – part2** | | | | |
| **Date:** 2023-05-15 | | | | |
| **Author(s):** | | | | |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Yanjun Sun | Qualcomm |  |  |  |
| Ali Raissinia |  |  |  |  |
| Steve Shellhammer |  |  |  |  |
| George Cherian |  |  |  |  |
|  |  |  |  |  |

Abstract

We propose the draft specification skeleton for NDP Announcement to help the creation of TGbk draft D0.1.

Revisions:

* Rev 0: Initial version of the document, using the text of 11.21.6.4.5-11.21.6.4.9 in 23/0390r3.
* Rev 1: incorporated suggested changes during the meeting (tagged by “r1” in the comments); Added new text on TXVECTOR parameter TXOP\_DURATION, renamed Secure LTF Parameters element and the Count field in it and other changes (tagged by “r1a” in the comments)

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbk 0.1 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbk D0.1 Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbk Editor: Editing instructions preceded by “TGbk Editor” are instructions to the TGbk editor to modify existing material in the TGbk draft. As a result of adopting the changes, the TGbk editor will execute the instructions rather than copy them to the TGbk Draft.***

**Discussion:**

The text is prepared for the following motion:

The Ranging NDP Announcement frame of 802.11bk will use the existing 320MHz indication of 802.11be:

* There is no change to the 802.11az Ranging NDP Announcement MAC content
* For a non-HT dup PPDU: set B7 in SERVICE field to 1 to indicate 320 MHz
* For an EHT MU PPDU: use the Bandwidth field in the U-SIG field to indicate 320 MHz

(11-23-48: 202301-12)

**Proposed spec text:**

***TGbk editor: Please note Baseline is REVme\_D2.1, IEEE 802.11az-2022 and IEEE 802.11be D3.1***

**11.21.6.4.5 Secure LTF in the TB and non-TB ranging measurement exchange protocol**

***Discussion****:*

*The HE-LTF Counter subfield in the Secure HE-LTF Parameters element looks reusable for EHT ranging NDP. Need group’s inputs on next step:*

1. *Rename them to “LTF Counter subfield” and “Secure LTF Parameters element” with a global replacement (assumed in this PDT, as “Secure LTF” has already been used in multiple figures in the baseline text) - - the group was supportive in this direction during the Apr 4th call, so we made change for this subclause in this direction*
2. *Keep the name as is*

*On secure EHT -LTF:*

1. *Expand the current subclauses - - the group was supportive in this direction during the Apr 4th call, so we made change for this subclause in this direction*
2. *Create separate subclauses*

***TGbk editor: please replace Secure HE-LTF Parameters element with Secure LTF Parameters element and HE-LTF Counter subfield with LTF Counter subfield throughout the spec, including Figure 9-788eu—Secure HE-LTF Parameters element format.***

**11.21.6.4.5.1 General**

Both the TB and the non-TB ranging measurement exchanges allow for the use of secure LTF for PHY security, if the ISTA and RSTA have established a secure LTF measurement setup as defined in [11.21.6.3.4](#H11o21o6o3o4) (Negotiation for secure LTF in the TB and non-TB measurement exchange). The frame exchange sequences stay nominally the same as described in [11.21.6.4.3](#H11o21o6o4o3) (TB ranging measurement exchange) and [11.21.6.4.4](#H11o21o6o4o4) (Non-TB ranging measurement exchange), except that the HE Ranging NDP , HE TB Ranging NDP, EHT Ranging NDP and EHT TB Ranging NDP will use secure LTF as described in  [[27.3.18a.1](#H27o3o18ao1)](#H27o3o18a) (HE Ranging NDP), [[27.3.18a.2](#H27o3o18ao2)](#H27o3o18b) (HE TB Ranging NDP), TBD (EHT Ranging NDP) and TBD (EHT TB Ranging NDP) respectively. To use the secure LTF the ISTA and RSTA need to share and communicate pseudorandom bit sequences that are used to generate and demodulate the secure LTF, the details and management thereof is described in the following.

**11.21.6.4.5.2 TB ranging measurement exchange with secure LTF**



**Figure 11-37o—Overview of the TB ranging measurement exchange with secure LTF**

An example of the negotiation and two TB Ranging Measurement Exchanges with secure LTF is shown in Figure [11-37o](#F11o37o) (Overview of TB ranging measurement exchange with secure LTF), where the LTF\_VALID\_SAC and SEC\_LTF\_CTR refer to the value of the values of the Validation SAC and Secure LTF Counter subfields. The first value of the Validation SAC and its associated Secure LTF Counter subfields shall be included in a protected IFTM frame, and thereafter any subsequent value of the Validation SAC and its corresponding Secure LTF Counter subfield shall be included in a protected R2I LMR frame. The value of the Validation SAC subfield shall also be the same value of the SAC subfield in the Trigger Dependent User Info field of the Secure Sounding Ranging Trigger frame. The description of how these fields are set in the TB ranging measurement exchange is given next.

In a TB ranging measurement exchange with secure LTF where there are multiple ISTAs involved in the measurement sequence, the RSTA shall transmit a Secure Sounding Ranging Trigger frame which includes a single User Info field to trigger a single ISTA at a time.

When an RSTA has established a secure LTF measurement exchange with an ISTA as specified in [11.21.6.3.4](#H11o21o6o3o4) (Negotiation for secure LTF in the TB and non-TB measurement exchange), the RSTA that sends a Secure Sounding Ranging Trigger frame to the STA shall set:

* The SAC subfield in the Trigger Dependent User Info field corresponding to the ISTA in the Secure Sounding Ranging Trigger frame to the same value as in the Validation SAC field in the Secure LTF Parameters element in the last transmitted protected IFTM, or last transmitted protected LMR frame, to the ISTA;

The RSTA shall set the I2R Rep subfield of the User Info field corresponding to the ISTA in the Secure Sounding Ranging Trigger frame equal to the value of the *RSTA Assigned I2R Rep* corresponding to the ISTA, where the value of the *RSTA Assigned I2R Rep* shall be greater than 0.

After transmission of the Secure Sounding Ranging Trigger frame to the ISTA, the RSTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS and LTF\_REP parameters set to the same values, respectively, as indicated by the SS Allocation and I2R Rep subfields of the User Info field;
* the LTF\_KEY and LTF\_IV parameters that are set to *ista-ltf-key* and *ltf-iv* for generating the secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);
* the TX\_WINDOW\_FLAG set to 1 if the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for I2R NDP; it is set to 0 otherwise,
* the LTF\_OFFSET set to 0.

When the RSTA receives the HE/EHT TB Ranging NDP from the ISTA, the RSTA shall:

1. Send a Ranging NDP Announcement frame.
2. Send an HE/EHT Ranging NDP with the TXVECTOR parameter LTF\_KEY and LTF\_IV set to the *rsta-ltf-key* and *ltf-iv* for generating secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation).
3. Send a protected LMR frame that includes the Secure LTF Parameters element to the ISTA.

Otherwise, the RSTA shall follow the rules in 10.22.2.2 (EDCA backoff procedure) as the frame exchange is not successful.

When an RSTA sends a Ranging NDP Announcement frame, it shall set the LTF Offset subfield in the STA Info fields to values that satisfy Equations [(11-6a)](#E11o6a) and [(11-6b):](#E11o6b)

(11-6a)

(11-6b)

where,

* Offset*n* represents the LTF Offset subfield value of the *nth* STA Info field in the Ranging NDP Announcement frame.
* *N\_STSn* represents the R2I NSTS subfield value plus 1 of the *nth* STA Info field in the Ranging NDP Announcement frame.
* *N\_LTFn* represents the number of LTF symbols based on *N\_STSn*, see Table 21-13 (Number of VHT-LTFs required for different numbers of space-time streams), for the *nth* STA Info field in the Ranging NDP Announcement frame.
* *Repn* represents the R2I Rep subfield value plus 1 of the *nth* STA Info field in the Ranging NDP Announcement frame.
* *MinOffset* represents the set of indexes of the STA Info fields of which the LTF Offset subfield values are less than the LTF Offset subfield value of *ith* STA Info field in the Ranging NDP Announcement frame.
* *MaxOffset* represents the set of indexes of all STA Info fields excluding *ith* STA Info field.

The RSTA shall set the R2I Rep subfield in each of the STA Info field in the Ranging NDP Announcement frame equal to the *RSTA Assigned R2I Rep* for each of the corresponding ISTAs, where all of the *RSTA Assigned R2I Rep* shall be greater than 0.

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame, received from the RSTA, the ISTA shall  
send an HE/EHT TB Ranging NDP with the TXVECTOR parameters LTF\_KEY and LTF\_IV that are set to *ista-ltf-key* and *ltf-iv* for generating the secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame, received from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame received from the RSTA, the ISTA shall send an HE/EHT TB Ranging NDP with the TXVECTOR parameters LTF\_KEY and LTF\_IV that are set to the *ista-ltf-key* and *ltf-iv* for generating any secure HE/EHT-LTF ;

When an ISTA receives a Ranging NDP Announcement frame from an RSTA in which the AID11 subfield in the STA Info field contains the 11 least significant bits of the AID or RSID of the ISTA, the ISTA shall issue a PHY-RXLTFSEQUENCE.request primitive with the following LTFVECTOR parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS, LTF\_REP, and LTF\_OFFSET parameters set to the same values, respectively, as indicated by the R2I NSTS, R2I Rep and LTF Offset subfields of the STA Info field addressed to it;
* the LTF\_KEY and LTF\_IV parameters that are set to the *rsta-ltf-key* and *ltf-iv* for generating the secure HE/EHT-LTFbased on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame received from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (General secure LTF octet stream generation), and;
* the TX\_WINDOW\_FLAG set to 1 if the ISTA and RSTA have negotiated to use the optional frequency domain Tx window for R2I NDP; it is set to 0 otherwise.

When an LMR frame contains range measurement results measured from an I2R NDP or an R2I NDP, an RSTA that transmits an R2I LMR frame, or when negotiated, an ISTA that transmits an I2R LMR frame, shall include the Secure LTF Parameters element in the protected LMR frame:

* The Measurement SAC subfield in the Secure LTF Parameters element in the protected LMR frame shall be set to the same value as in the SAC subfield in the Trigger Dependent User Info field in the Secure Sounding Ranging Trigger destined to the ISTA receiving or transmitting this protected LMR frame.
* The Measurement Result LTF Offset subfield in the Secure LTF Parameters element in the protected LMR frame shall be set to the same value as in the LTF Offset subfield of the STA Info field in the Ranging NDP Announcement frame that preceded the R2I NDP destined to the ISTA for this measurement result.

When an ISTA or RSTA receives the R2I or I2R protected LMR frame, the ISTA or RSTA shall compare the value of the Measurement Result LTF Offset subfield with the value of the LTF Offset subfield in the corresponding STA Info field of the Ranging NDP Announcement frame, and if these two values don’t match, the ISTA or RSTA shall discard the measurement results carried in the protected LMR frame.

When a frame exchange that consists of receiving an HE/EHT TB Ranging NDP and transmitting HE/EHT Ranging NDP results into a Null-SAC-LTF, the RSTA shall not use the TOA and TOD value of the HE/EHT TB Ranging NDP and HE/EHT Ranging NDP respectively and shall set the Invalid Measurement Indication subfield to 1 in the TOA error field in the protected LMR carrying the TOA value of the I2R HE/EHT TB Ranging NDP.

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame received from the RSTA, the ISTA shall:

* not use the TOD value of the I2R HE/EHT TB Ranging NDP
* not use the TOA value of the R2I HE/EHT Ranging NDP, and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the protected LMR carrying the TOA value of the HE/EHT Ranging NDP if the I2R LMR transmission from the ISTA was negotiated.

The STA shall discard the SAC value used in the frame exchange and shall not use the same SAC value in the current measurement exchange.

NOTE—In TB ranging measurement exchange with secure LTF, the RSTA never sends the SAC subfield with value 0 in the Trigger Dependent User Info field in the Secure Sounding Ranging Trigger frame.

When there is a transmission failure within a secure measurement exchange sequence, the recovery procedure of the LTF\_VALID\_SAC and its associated SEC\_LTF\_CTR parameters is illustrated in Figure [11-37p](#F11o37p) (Error recovery of TB ranging measurement exchange using secure LTF).



***TGbk editor: Please delete the 2 occurances of “HE” in the figure above***

**Figure 11-37p—Error recovery of TB ranging measurement exchange using secure LTF**

**11.21.6.4.5.3 Non-TB ranging measurement exchange with secure LTF**



**Figure 11-37q—Overview of the non-TB ranging measurement exchange with secure LTF**

An overview of the negotiation and two non-TB ranging measuerment exchanges are illustrated in Figure [11-37q](#F11o37q) (Overview of non-TB ranging measurement exchange with secure LTF). The LTF\_VALID\_SAC and its associated SEC\_LTF\_CTR parameter shall be included in a protected IFTM frame and a protected R2I LMR frame. The LTF\_VALID\_SAC shall also be included in the SAC subfield in the Ranging NDP Announcement frame. The detailed description of how the fields in these frames are set follows.

When an ISTA has established a secure LTF measurement exchange with an RSTA as specified in [11.21.6.3.4](#H11o21o6o3o4) (Negotiation for secure LTF in the TB and non-TB ranging measurement exchange), this ISTA shall set the following subfields in any Ranging NDP Announcement frame addressed to that RSTA as follows:

* The SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame is set to the same value contained in the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected R2I LMR frame, received from the RSTA;
* Otherwise the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame is set to a value of 0 to indicate that a new SEC\_LTF\_CTR and the corresponding LTF\_VALID\_SAC parameter are needed.

The ISTA shall set the I2R Rep subfield and R2I Rep subfield of the STA Info field in the Ranging NDP Announcement frame to the values of *RSTA Assigned I2R Rep* and the *RSTA Assigned R2I Rep* respectively, corresponding to the RSTA. Both values of the *RSTA Assigned R2I Rep,* and *RSTA Assigned I2R Rep,* shall begreater than 0.

An ISTA that sends an I2R NDP a SIFS after transmission of the Ranging NDP Announcement frame shall set the TXVECTOR parameters LTF\_KEY and LTF\_IV as follows:

* Either to the value of Null-SAC-LTF, if the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame, is equal to 0 ;
* Or the *ista-ltf-key* and *ltf-iv* for generating secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame, received from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation).

After transmission of the Ranging NDP Announcement frame to the RSTA, the ISTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with an LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the R2I NSTS and R2I Rep subfields in the STA Info field with the AID11 subfield less than or equal to 2007;
* the LTF\_KEY and LTF\_IV parameters that are set to either to the value of Null-SAC-LTF, if the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame is equal to 0; Or the *rsta-ltf-key* and *ltf-iv* for generating a secure HE/EHT-LTF based on the values of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame received, from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);
* the TX\_WINDOW\_FLAG set to 1 if the ISTA and RSTA have negotiated to use the optional frequency domain Tx window for R2I NDP; it is set to 0 otherwise, and
* the LTF\_OFFSET set to 0.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the SAC subfield in the STA Info field with AID11 equal to 2043 is not equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA, the RSTA shall:

* Send an HE/EHT Ranging NDP to the ISTA with the TXVECTOR parameters r*sta-ltf-key* and *ltf-iv* for generating any secure LTF to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame;
* Send a protected LMR frame with a Secure LTF Parameters element containing the SEC\_LTF\_CTR and the corresponding LTF\_VALID\_SAC parameters to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the value of the SAC subfield in the STA Info field with AID11 equal to 2043 is equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA, the RSTA shall:

* Send an HE/EHT Ranging NDP with the TXVECTOR parameters *rsta-ltf-key* and *ltf-iv* for generating a secure HE/EHT-LTF based on the values of the Secure LTF Counter in the Secure LTF Parameters element in the last transmitted protected IFTM frame, or last transmitted protected LMR frame to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);
* Send a protected LMR frame that includes the Secure LTF Parameters element to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA, the RSTA shall also issue a PHY-RXLTFSEQUENCE.request primitive with an LTFVECTOR with the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the I2R NSTS and I2R Rep subfields in the STA Info field with the AID11 subfield less than or equal to 2007;
* the LTF\_KEY and LTF\_IV parameters that are set to the i*sta-ltf-key* and *ltf-iv* for receiving a secure HE/EHT-LTF based on the values of the Secure LTF Counter and corresponding Validation SAC subfields in the Secure LTF Parameters element in the last transmitted protected IFTM frame, or last transmitted protected LMR frame to the ISTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (General secure LTF octet stream generation);
* the TX\_WINDOW\_FLAG set to 1 if the ISTA and RSTA have negotiated to use the optional frequency domain Tx window for I2R NDP; it is set to 0 otherwise, and;
* the LTF\_OFFSET set to 0.

An RSTA transmitting an R2I LMR frame, or an ISTA when negotiated to transmit LMR frame, containing range measurement results measured from an I2R NDP and a R2I NDP, shall include the Secure LTF Parameters element in the protected LMR frame and set the Measurement SAC subfield in the Secure LTF Parameters element in the protected LMR frame to the same value as in the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP.

When a STA sends a Null-SAC-LTF in an HE/EHT Ranging NDP**,** the STA shall not use the TOD value of the HE/EHT Ranging NDP for the secure range measurement exchange.

When a STA receives a Null-SAC-LTF in an HE/EHT Ranging NDP, the STA shall not use the TOA value of the HE/EHT Ranging NDP, and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the protected LMR carrying the TOA value of the HE/EHT Ranging NDP.

When there is a transmission failure within a secure measurement exchange, the recovery procedure of the LTF\_VALID\_SAC is illustrated in Figure [11-37r](#F11o37r) (Error recovery of non-TB ranging measurement exchange using secure LTF).

A STA shall discard the LTF\_VALID\_SAC parameter used in the frame exchange and shall not use the same LTF\_VALID\_SAC parameter in the current measurement exchange.



***TGbk editor: Please delete the 2 occurances of “HE” in the figure above***

**Figure 11-37r—Error recovery non-TB ranging measurement exchange using secure LTF**

11.21.6.4.5.4 Overview of secure LTF octet stream generation

This clause describes mechanisms for generating the SAC, LTF protection keys, counters, and the pseudorandom octet stream used to randomize the input to the modulation and per stream phase rotation for constructing secure LTFs. The mechanism is illustrated in Figure [11-37s](#F11o37s) (ISTA secure LTF octet stream generation, and Figure [11-37t](#F11o37t) (RSTA secure LTF octet stream generation).

For each secure measurement (e.g. NDP exchanges), a SAC and two secret keys *ista-ltf-key* and *rsta-ltf-key* shall be derived by the ISTA and the RSTA independently as follows.

SAC-and-LTF-Keys = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure HE-LTF Expansion”, Secure-LTF-Counter)

Where

* KDF and Hash are the key derivation function and hash function determined by the AKM used to derive the PTKSA from which the Secure-LTF-Key-Seed was derived.
* Length is equal to 272 (bits)
* SAC = L(SAC-and-LTF-Keys, 0, 16)
* *ista-ltf-key* = L(SAC-and-LTF-Keys, 16, 128)
* *rsta-ltf-key* = L(SAC-and-LTF-Keys, 144, 128)

The *ista-ltf-key* shall be used to generate the pseudorandom octet stream to protect all of the LTFs in PPDUs transmitted by the ISTA. The *rsta-ltf-key* shall be used to generate the pseudorandom octet stream to protect all of the LTFs in PPDUs transmitted by the RSTA. The ISTA and RSTA shall use the same derivation and derive identical keys.

With the SAC constructed as above, an attacker not knowing the Secure-LTF-Key-Seed would not be able to predict the SAC that would be used for a given measurement.

Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 shall be used to encode the value of the Secure LTF Counter subfield in the KDF as well as in the transmitted LTF sequence information. The counter shall be padded with leading (MSB) 0s to be exactly 6 octets.

The 16-octet IV input *ltf-iv* to the secure LTF bit generator shall be constructed as follows:

* First 6 octets shall be the transmitter MAC address (A2).
* Next 6 octets shall encode the value of the Secure LTF Counter subfield with the encoding convention described above.
* Final 4 octets shall be used as a 32-bit block counter. The block counter shall be initialized to 0 before the NDP with secure LTFs is transmitted or received. The counter shall be incremented by 1 each time an AES block is output by the generator.

Each time pseudorandom bits are required to protect the LTFs in an NDP, the secure LTF bit generator generates the required number of AES blocks using the AES algorithm (see FIPS PUB 197) with the corresponding 128-bit key and 128-bit IV inputs. The output of the AES-128 counter encryption is a 128-bit integer. It shall be converted using the conventions specified in 12.4.7.2.2 (Integer to octet string conversion) to obtain the octet stream used for secure LTF generation.

NOTE— A 6 octet parameter representing the value of the Secure LTF Counter subfield is sufficient because a unicast protected management frame that uses a 6 octet PN is used to convey the LTF sequence information that carries the counter.

NOTE—The pseudorandom bit generator is based on AES-128 Counter mode approved by NIST (CTR-DRBG - NIST SP 800 90Ar1 - Recommendations for Random Number Generation).

The number of pseudorandom bits that can be generated without violating security guarantees of the scheme is 2^39 without updating the key or reseeding the generator with additional entropy.

Secure LTF measurement requires a variable number of octets from the pseud random octet stream depending on the TXVECTOR or RXVECTOR parameters for the LTFs as described in section [27.3.18b.2](#H27o3o18bo2) (Generation of a randomized secure LTF sequence). The initial block counter value used to construct the *ltf-iv* for setting the TXVECTOR and RXVECTOR parameters shall be 0.

**11.21.6.4.5.5 Secure LTF octet stream generation on an ISTA**

Figure [11-37s](#F11o37s) (ISTA secure LTF octet stream generation) illustrates the scheme for generating the SAC, LTF protection keys, and counter values used to generate a pseudorandom octet stream on an ISTA.

Diagram

Description automatically generated

***TGbk editor: Please replace “*Secure LTF Expansion*” with “*Secure HE-LTF Expansion*” in the figure above***

**Figure 11-37s—ISTA secure LTF octet stream generation**

For each secure measurement on an ISTA, the following parameters shall be used for generating the pseudorandom octet stream used to construct the LTFs for NDPs:

* the *ista-ltf-key* and *rsta-ltf-key* for transmitted NDP (TXVECTOR parameter LTF\_KEY) and received NDP (RXVECTOR parameter LTF\_KEY) respectively.
* the *ltf\_iv* for transmitted NDP (TXVECTOR parameter LTF-IV) and received NDP (RXVECTOR parameter LTF-IV) with corresponding ISTA MAC address and RSTA MAC address respectively together with the value of the Secure LTF Counter subfield and the block counter

**11.21.6.4.5.6 Secure LTF input octet stream generation on an RSTA**

The following Figure [11-37t](#F11o37t) (RSTA secure LTF octet stream generation) illustrates the scheme for generating the SAC, LTF protection keys, and counter values used to generate a pseudorandom octet stream on an RSTA.

Diagram

Description automatically generated

***TGbk editor: Please replace “*Secure LTF Expansion*” with “*Secure HE-LTF Expansion*” in the figure above***

**Figure 11-37t—RSTA secure LTF octet stream generation**

For each secure measurement on an RSTA, the following parameters are provided for generating the pseudorandom octet stream to construct the LTFs for NDPs:

* the *ista-ltf-key* and *rsta-ltf-key* for received NDP (RXVECTOR parameter LTF\_KEY) and transmitted NDP (TXVECTOR parameter LTF\_KEY) respectively.
* the *ltf\_iv* for received NDP(RXVECTOR parameter LTF-IV) and for transmitted NDP (TXVECTOR parameter LTF-IV) with corresponding ISTA MAC address and RSTA MAC address respectively together with the values of the Secure LTF Counter subfield and the block counter.

NOTE—In an R2I NDP used for range measurement, LTFs assigned to each of the recipient STAs would use their corresponding pseudorandom octet stream derived from the key material from the corresponding PTKSA for the recipient.

The values of the Secure LTF Counter subfield shall be maintained for the lifetime of a PTKSA used for secure LTF measurements. It shall not be reset between measurements and shall not be reset for multiple FTM negotiations using the same PTKSA.

The values of the Secure LTF Counter subfield used for each measurement protected bits is derived from a given Secure-LTF-Key-Seed (and its KDK and the PTKSA) and shall be unique. When the derived SAC is equal to 0, the RSTA shall increment the secure LTF counter parameter by 1 and derive the SAC until a nonzero SAC value is obtained. An RSTA shall also increment the secure LTF counter parameter by 1 each time an *ista-ltf-key* and *rsta-ltf-key* are derived.

**11.21.6.4.6 Transmission of a ranging NDP**

An RSTA transmitting an HE Ranging NDP or EHT Ranging NDP to one or more peer ISTAs shall set the TXVECTOR parameter as follows:

* The FORMAT parameter is set as follows:
  + Is set to EHT\_MU if the CH\_BANDWIDTH is equal to 320 MHz
  + Is set to HE\_SU otherwise
* The RANGING\_FLAG is present
* The UPLINK\_FLAG parameter is set to 0
* The APEP\_LENGTH parameter is set to 0
* The SECURE\_LTF\_FLAG is set as follows:
  + Is set to 0 in the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)) and non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)).
  + Is set to 1 in the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)) and the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)).
* The TX\_WINDOW\_FLAG is set to 1 if the SECURE\_LTF\_FLAG is set to 1 and the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for R2I NPDs; it is set to 0 otherwise.
* In the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)), the NUM\_USERS parameter is set to the number of ISTAs that the HE/EHT Ranging NDP is transmitted to.
* In the Non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)), the TXPWR\_LEVEL\_INDEX parameter is set to a value that matches the Tx Power value indicated in the R2I NDP Tx Power field in the following LMR frame, except if the value in the R2I NDP Tx Power field was set to a reserved value.
* If the FORMAT parameter is set to HE\_SU, the DOPPLER parameter is set to 0
* The NUM\_STS parameter is set as follows:
  + In the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)), set to the same value as the R2I NSTS subfield in the STA Info field in the preceding Ranging NDP Announcement frame plus 1.
  + In the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)).
    - The NUM\_STS[*p*] is set to the same value as the R2I NSTS subfield in the STA Info field addressed to the corresponding STA *p* in the preceding Ranging NDP Announcement frame plus 1 when the HE/EHT Ranging NDP is transmitted to more than one ISTA.
    - The NUM\_STS is set to the same value as the R2I NSTS subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1, when the HE/EHT Ranging NDP is transmitted to one ISTA.
  + In the Non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) and the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)), set to the same value as the R2I NSTS subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1.
* The LTF\_REP parameter is set as follows:
  + In the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)), set to the same value as the R2I Rep subfield in the STA Info field in the preceding Ranging NDP Announcement frame plus 1.
  + In the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)):
    - The LTF\_REP[*p*] is set to the same value as the R2I Rep subfield in the STA Info field addressed to the corresponding STA *p* in the preceding Ranging NDP Announcement frame plus 1 when the HE/EHT Ranging NDP is transmitted to more than one ISTA.
    - The LTF\_REP is set to the same value as the R2I Rep subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1 when the HE/EHT Ranging NDP is transmitted to one ISTA.
  + In the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) and the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)), set to the same value as the R2I Rep subfield in the STA Info field with AID11 subfield less than or equal to 2007 in the preceding Ranging NDP Announcement frame plus 1.
* The CH\_BANDWIDTH parameter is set as follows:
  + In the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)), and TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)), set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging Sounding Trigger frame
  + In the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) and non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)), set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging NDP Announcement frame
* In the TB and non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5](#H11o21o6o4o5)), the LTF\_KEY parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (TB ranging measurement exchange with secure LTF) and [11.21.6.4.5.3](#H11o21o6o4o5o3) (Non-TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_KEY parameter is not present.
* In the TB ranging measurement exchange with secure LTF, the LTF\_OFFSET parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_OFFSET parameter is not present.
* If the FORMAT parameter is set to HE\_SU, the HE\_LTF\_TYPE parameter is set to 2xHE-LTF
* If the FORMAT parameter is set to EHT\_MU the EHT\_LTF\_TYPE parameter is set to 2xEHT-LTF
* The GI\_TYPE parameter is set to 1u6s\_GI
* The SPATIAL\_REUSE parameter is set to SRP\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED
* The BSS\_COLOR parameter is set to the value indicated in the BSS Color subfield of the HE Operation element transmitted by the RSTA
* If the FORMAT parameter is set to HE\_SU, the TXOP\_DURATION parameter is set to either 127 or a value defined in Equation (26-3), replacing *D*HE\_NDPA by *D*Ranging\_NDP\_Announcement which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcementframe.
* If the FORMAT parameter is set to EHT\_MU, the TXOP\_DURATION parameter is set to either 127 or a value defined in Equation (35-2), replacing *D*EHT\_NDPA by *D*Ranging\_NDP\_Announcement which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcementframe.

An ISTA transmitting an HE Ranging NDP or EHT Ranging NDP shall set the TXVECTOR parameter as follows:

* The FORMAT parameter is set as follows:
  + Is set to EHT\_MU if the CH\_BANDWIDTH is equal to 320 MHz
  + Is set to HE\_SU otherwise
* The RANGING\_FLAG is present
* The UPLINK\_FLAG parameter is set to 1
* The APEP\_LENGTH parameter is set to 0
* The SECURE\_LTF\_FLAG is set as follows:
  + Is set to 0 in the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)).
  + Is set to 1 in the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)),
* The TX\_WINDOW\_FLAG is set to 1 if the SECURE\_LTF\_FLAG is set to 1 and the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for I2R NPDs; it is set to 0 otherwise.
* If the FORMAT parameter is set to HE\_SU, the DOPPLER parameter is set to 0
* The NUM\_STS parameter is set to the same value as the I2R NSTS subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1.
* The LTF\_REP parameter is set to the same value as the I2R Rep subfield with AID11 subfield equal or less than 2007 in the STA Info field in the preceding Ranging NDP Announcement frame plus 1.
* The TXPWR\_LEVEL\_INDEX parameter is set to a value that matches the Tx Power value indicated in the I2R NDP Tx Power subfield in the STA Info field with the AID11 subfield set to 2045 in the preceding Ranging NPD Announcement frame, except if the value in the I2R NDP Tx Power subfield was set to a reserved value.
* The CH\_BANDWIDTH set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging NDP Announcement frame
* In the non-TB ranging measurement exchange with secure LTF, the LTF\_KEY parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (Non-TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_KEY parameter is not present
* If the FORMAT parameter is set to HE\_SU, the HE\_LTF\_TYPE parameter is set to 2xHE-LTF
* If the FORMAT parameter is set to EHT\_MU, the EHT\_LTF\_TYPE parameter is set to 2xEHT-LTF
* The GI\_TYPE parameter is set to 1u6s\_GI
* The SPATIAL\_REUSE parameter is set to SRP\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED
* The BSS\_COLOR parameter is set to the value indicated in the BSS Color subfield of the HE Operation element received from the RSTA
* If the FORMAT parameter is set to HE\_SU, the TXOP\_DURATION parameter is set to either 127 or a value defined in Equation (26-3), replacing *D*HE\_NDPA by *D*Ranging NDP Announcement which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcementframe.
* If the FORMAT parameter is set to EHT\_MU, the TXOP\_DURATION parameter is set to either 127 or a value defined in Equation (35-2), replacing *D*EHT\_NDPA by *D*Ranging\_NDP\_Announcement which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcementframe.

An ISTA transmitting an HE TB Ranging NDP or an EHT TB Ranging NDP to an RSTA shall set the TXVECTOR parameter as follows:

* The FORMAT parameter is set as follows:
  + Is set to EHT\_TB if the CH\_BANDWIDTH is equal to 320 MHz
* Is set to HE\_TB otherwiseThe RANGING\_FLAG is present
* The APEP\_LENGTH parameter is set to 0
* The SECURE\_LTF\_FLAG is set as follows:
  + Is set to 0 in the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)).
  + Is set to 1 in the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)).
* The TX\_WINDOW\_FLAG is set to 1 if the SECURE\_LTF\_FLAG is set to 1 and the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for I2R NPDs; it is set to 0 otherwise.
* If the FORMAT parameter is set to HE\_TB, the DOPPLER parameter is set to 0
* The NUM\_STS parameter is set to the same value as the Number Of Spatial Streams subfield in the SS Allocation field in the User Info field in the preceding Ranging Sounding Trigger frame.
* The LTF\_REP parameter is set to the same value as the I2R Rep subfield in the User Info field in the preceding Ranging Sounding Trigger frame plus 1.
* The CH\_BANDWIDTH parameter is set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging Sounding Trigger frame
* In the TB ranging measurement exchange with secure LTF, the LTF\_KEY parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_KEY parameter is not present
* If the FORMAT parameter is set to HE\_TB, the HE\_LTF\_TYPE parameter is set to 2xHE-LTF
* If the FORMAT parameter is set to EHT\_TB, the EHT\_LTF\_TYPE parameter is set to 2xEHT-LTF
* The GI\_TYPE parameter is set to 1u6s\_GI
* The SPATIAL\_REUSE parameter is set to SRP\_AND\_NON-SRG\_OBSS\_PD\_PROHIBITED
* The BSS\_COLOR parameter is set to the value indicated in the BSS Color subfield of the HE Operation element received from the RSTA

If the FORMAT parameter is set to HE\_TB, the TXOP\_DURATION parameter is set as defined in 26.11.5 (TXOP\_DURATION). If the FORMAT parameter is set to EHT\_TB, the TXOP\_DURATION parameter is set as defined in 35.11.1.5 (TXOP\_DURATION).

**11.21.6.4.7 Time of arrival estimationusing phase shift feedback**

Based on Figure [11-37u](#F11o37u) (Timing diagram of a Measurement Sounding phase in TB ranging based on phase shift of I2R NDP or R2I PPDUs), and Equation [(11-6e)](#E11o6e) , to enable the ISTA to derive the RTT, the RSTA needs to compute TOA t2 and feed t2 and t3 back to ISTA using R2I LMR. Instead of utilizing TOA t2 for RTT computation, a phase shift feedback can be prepared by RSTA and fed back to ISTA for deriving RTT.



**Figure 11-37u—Timing diagram of a measurement sounding phase in TB ranging based on phase shift of I2R NDP and R2I NDP PPDUs**

As shown in Figure [[11-37u](#F11o37u)](#F11o37s) (Timing diagram of a Measurement Sounding phase in TB ranging based on phase shift of I2R NDP and R2I NDP PPDUs), in the phase shift feedback method, the ISTA transmits an I2R NDP at TOD t1, and the RSTA determines the phase shift tp2 of the I2R NDP. The RSTA transmits a R2I NDP at TOD t3, and the ISTA determines the phase shift tp4 and TOA t4 of the R2I NDP. tp2 and tp4 are determined from the phase slope of the frequency domain channel estimation of the corresponding NDP. An example of calculation of the phase shift is shown in Annex AD.1.

The RSTA sends the R2I NDP at TOD t3, and after receiving the R2I NDP, the ISTA calculates the phase shift tp4 and TOA t4 of R2I NDP. The value of tp2 and tp4 are calculated utilizing the frequency domain channel estimation of I2R NDP and R2I NDP.

The phase shift is defined as the average linear phase shift between two adjacent tones normalized by the tone spacing. To enable the ISTA calculates the RTT, the RSTA should feed phase shift tp2 and TOD t3 back to the ISTA using R2I LMR, and the ISTA can calculate the RTT as:

RTTISTA = (t4 – t1) – (t3 – t2’’), with t2’’ = tp2 – (tp4 – t4) (11-6e)

When the I2R LMR with phase shift feedback is negotiated between ISTA and RSTA, I2R LMR carries phase shift tp4 and TOD t1, and then the RSTA can calculate the RTT as:

RTTRSTA = (t4’’ – t1) – (t3 – t2), with t4’’ = tp4 – (tp2 – t2)  (11-6f)

**11.21.6.4.8 Measurement exchange in passive TB ranging mode**

**11.21.6.4.8.1 General**

As stated in [11.21.6.1.3](#H11o21o6o1o3) (Passive TB ranging), the passive TB ranging mode is a variant of the TB ranging mode. In all aspects, except where explicitly stated differently, the passive TB ranging mode, its protocols, procedures, components, and definitions follow the rules for TB ranging mode.

In particular the measurement exchanges for passive TB ranging follows the rules and procedures described in [11.21.6.4.3](#H11o21o6o4o3) (TB ranging measurement exchange), with subclauses, unless explicitly stated otherwise.

In passive TB ranging, the RSTA shall transmit the Passive Sounding Ranging Trigger frame instead of the Sounding Ranging Trigger frame. Upon receiving of the Passive Sounding Ranging Trigger frame, if the bandwidth indicated by the frame is less than or equal to 160 MHz, the ISTA shall respond with an HE Ranging NDP instead of an HE TB Ranging NDP; if the bandwidth indicated by the frame is equal to 320 MHz, the ISTA shall respond with an EHT Ranging NDP instead of an EHT TB Ranging NDP; see [11.21.6.4.8.3](#H11o21o6o4o8o3) (Passive TB ranging measurement sounding phase) for further details.

Furthermore, the RSTA shall broadcast two frames, the Primary and Secondary RSTA Broadcast Passive TB Ranging Measurement Report frames containing measurement data and related information; see [11.21.6.4.8.4](#H11o21o6o4o8o4) (Passive TB ranging measurement reporting phase) for further details.

The passive TB ranging exchanges shall only occur in an availability window assigned for Passive TB ranging.

For passive TB ranging, the timestamps reported within each availability window shall be derived from a clock that runs continuously during the availability window.

If there is a discontinuity in the clock for the FTM timestamping between two reported TOD timestamps, then the TOD Not Continuous subfield in the Timestamp Error subfield of the Timestamp Measurement Report subfield in the ISTA Passive TB Ranging Measurement Report element shall be set to 1. Otherwise it shall be set to 0.

**11.21.6.4.8.2 Polling Phase of passive TB ranging**

The Polling phase of passive TB ranging follows the same rules and procedures for the Polling phase of TB ranging described in Subclause [11.21.6.4.3.2](#H11o21o6o4o3o2) (Polling Phase of TB ranging).

**11.21.6.4.8.3 Passive TB ranging measurement sounding phase**

The passive TB ranging measurement sounding follows the same rules and procedures for the measurement sounding for TB ranging described in [11.21.6.4.3.3](#H11o21o6o4o3o3) (TB ranging Measurement Sounding phase), unless explicitly stated otherwise.

The second phase of the passive TB ranging measurement sequence, after the passive TB ranging Polling phase, is called the passive TB ranging measurement sounding phase. The passive TB ranging measurement sounding phase may include one or more Passive Sounding Ranging Trigger frames and HE/EHT Ranging NDP exchanges, a Ranging NDP Announcement frame, and an HE/EHT Ranging NDP transmission; see Figure [11-37v](#F11o37v) (Passive TB ranging polling, Measurement Sounding, and Measurement Reporting phases).



**Figure 11-37v—Passive TB ranging polling, measurement sounding, and measurement reporting phases.**

In passive TB ranging, for each ISTA, the RSTA shall transmit a Passive Sounding Ranging Trigger frame, which includes a single User Info field.

An RSTA shall transmit one or more Passive Sounding Ranging Trigger frames, each of which is addressed to a single ISTA, the first one coming a SIFS time after the TB Polling phase.

An ISTA addressed by the AID/RSID in the Passive Sounding Ranging Trigger frame shall transmit an HE/EHT Ranging NDP a SIFS time after the reception of the Passive TB Ranging Ranging Trigger frame.

An RSTA transmitting a Passive Sounding Ranging Trigger frame shall not use a bandwidth wider than that indicated in the IFTM frame sent to the ISTA, and the RSTA shall set the TXVECTOR parameter CH\_BANDWIDTH to be the same value as the UL BW subfield of the Common Info field in the Passive Sounding Ranging Trigger frame.

NOTE—Generally a PSTA benefits from consistent ranging measurement performance when an RSTA initiates a passive TB ranging sequence with the nominal advertised bandwidth in every TXOP.

An RSTA transmitting a Ranging NDP Announcement frame and an HE/EHT Ranging NDP after receiving an HE/EHT Ranging NDP as a response to a Passive Sounding Ranging Trigger frame shall set the TXVECTOR parameter CH\_BANDWIDTH to be the same value as the BW subfield of the Common Info field in the Passive Sounding Ranging Trigger frame.

An ISTA transmitting an HE/EHT Ranging NDP as a response to a Passive Sounding Ranging Trigger frame shall set the TXVECTOR parameter CH\_BANDWIDTH to be the same value as the UL BW subfield of the Common Info field in the Passive Sounding Ranging Trigger frame.

If the CH\_BANDWIDTH of the Ranging NDP, either the I2R NDP or the R2I NDP, is equal to 320 MHz, the corresponding NDP shall be an EHT Ranging NDP and the R2I LMR in the corresponding measurement exchange sequence shall be transmitted in an EHT MU PPDU. Otherwise, the corresponding NDP shall be an HE Ranging NDP and the R2I LMR shall be transmitted in an HE MU PPDU.

As in TB ranging, an ISTA participating in a passive TB ranging exchange shall measure the TOD of its own HE/EHT Ranging NDP and either the TOAs, or both the TOAs and the phase shift feedback TOAs (PSTOAs), when it receives the RSTA’s HE/EHT Ranging NDP. In addition, optionally the ISTA may also measure and report either the TOAs, or both the TOAs and the PSTOAs, when it receives the HE/EHT Ranging NDPs transmitted by the other ISTAs participating in the passive TB ranging exchange. By reporting the timestamps for when it received the other ISTAs NDP transmissions, the quality of the location estimate for a PSTA listening in to the passive TB ranging exchanges can be improved.

The number of NSTS used in the passive TB ranging exchanges shall be less than or equal to 4.

When phase shift feedback is negotiated between an ISTA and an RSTA in passive TB ranging, the protocol for the measurement sounding phase differs from passive TB ranging with TOA feedback on the following points:

* The RSTA shall measure phase shift feedback TOA (PSTOA), in addition to measuring the TOA, on the I2R NPD it receives from the ISTA.
* The ISTA shall measure:  
  + the phase shift TOA (PSTOA), in addition to measuring the TOA, for the R2I NDP it receives from the RSTA,
  + and may also measure phase shift TOA(s) (PSTOAs), in addition to measuring the TOA(s), for the I2R NDP(s) it receives from other ISTA(s).

See Figure [11-37w](#F11o37w) (Example Timing diagram of a Measurement Sounding phase in passive TB ranging) for an example of timestamps measured by the RSTA, ISTA and a PSTA in a passive TB ranging measurement exchange. The timestamp values t1, t2, t3 and t4 are analogous to the corresponding labeled timestamps in [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement Sounding phase of TB ranging). The timestamps t5 and t6 are the times at which the I2R NDP and R2I NDPs arrive at the PSTA, respectively.



**Figure 11-37w—Example timing diagram of a measurement sounding phase in passive TB ranging**

The PSTA may use the ISTA’s and RSTA’s timestamps, together with its own measured TOAs of the ranging NDPs, t5 and t6, to calculate its differential time of flight to the RSTA and the ISTA.

The differential time-of-flight (DToF) from PSTA to RSTA and ISTA (DToF\_PRI) is defined by Equation [(11-6g)](#E11o6g).

DToF\_PRI = ToF\_PR – ToF\_PI, (11-6g)

Where, ToF\_PR is the time of flight between the PSTA and the RSTA, and ToF\_PI is the time of flight between the PSTA and the ISTA. The differential time of flight DToF\_PRI can be computed as per Equation [(11-6h)](#E11o6h):

DToF\_PRI = t6 – t5 – 0.5 × t3’ + 0.5 × t2’ – 0.5 × t4’ + 0.5 × t1’, (11-6h)

where,

t1’ and t4’ are the time at which the I2R NDP was transmitted from the ISTA and the time at which the R2I NDP was received by the ISTA, respectively, converted by the PSTA from the ISTA’s time basis to the PSTA’s time basis.

t2’ and t3’ are the time at which the I2R NDP was received by the RSTA and the time at which the R2I NDP was transmitted by the RSTA, respectively, converted by the PSTA from the RSTA’s time basis to the PSTA’s time basis.

At the PSTA, the mechanism by which t1’ and t4’ is derived from t1, t4, the ISTA’s reported CFO, and the PSTA’s CFO measured with respect to the RSTA, is implementation dependent.

At the PSTA, the mechanism by which t2’ and t3’ is derived from t2, t3, and the PSTA’s CFO measured with respect to the RSTA, is implementation dependent.

By multiplying the differential time of flight, DToF\_PRI, with the speed of light, the differential distance from PSTA to RSTA and ISTA can be computed.

See [11.21.6.4.8.5](#H11o21o6o4o8o5) (Passive TB ranging differential time-of-flight calculations using phase shift TOA timestamps) for how the PSTA’s differential distance to the RSTA and the ISTA can be computed using PSTOAs measured by the RSTA and the ISTA.

**11.21.6.4.8.4 Passive TB ranging measurement reporting phase**

The passive TB ranging measurement reporting follows the same rules and procedures for the measurement reporting for TB ranging described in [11.21.6.4.3.4](#H11o21o6o4o3o4) (TB ranging Measurement Sounding phase), unless explicitly stated otherwise.



**Figure 11-37x—Passive TB ranging measurement reporting phase**

The last phase of the passive TB ranging measurement sequence is the passive TB ranging measurement reporting phase and occurs a SIFS time after the passive TB ranging measurement sounding phase; see Figure [11-37x](#F11o37x) (Passive TB ranging measurement reporting phase) for a depiction of the passive TB ranging measurement reporting phase.

In the passive TB ranging measurement reporting phase, an RSTA shall send a Passive TB Ranging Measurement Report frame and the Report Ranging Trigger frame to one or more ISTAs that sent an HE/EHT Ranging NDP in the preceding passive TB ranging measurement sounding phase. An ISTA addressed by the Report Ranging Trigger frame shall transmit an ISTA Passive TB Ranging Measurement Report frame a SIFS time after the Report Ranging Trigger frame transmission to report its I2R LMR.

In order to facilitate broadcasting of the ISTA’s timestamps by the RSTA the ISTA Passive TB Ranging Measurement Report frame shall be transmitted as a public Action frame.

The ISTA Passive TB Ranging Measurement Report element, see [[[[9.4.2.304](#H09o4o2o304)](#H09o4o2o304)](#H09o4o2o304)](#H09o4o2o302) (ISTA Passive TB Ranging Measurement Report element), in ISTA Passive TB Ranging Measurement Report frames shall contain:

* a Sounding Dialog Token Number identifying the measurement sounding phase in which the reported ISTA’s timestamps were measured;
* the CFO of the ISTA with respect to the RSTA;
* the TOD timestamp for the I2R NDP that the ISTA transmitted – labeled with the AID12/RSID12 of the ISTA;
* the TOA, timestamp for the R2I NDP that the ISTA received from the RSTA;
* optionally, the TOA timestamps for the I2R NDPs received from other ISTAs participating in the passive TB ranging (i.e. polling, sounding and reporting triplet) identified by the Sounding Dialog Token Number – labeled with their respective AID12/RSID12s.

If phase shift TOA reporting has been negotiated, the ISTA Passive TB Ranging Measurement Report element shall also include:

* the PS-TOA timestamp of the R2I NDP that the ISTA received from the RSTA; and
* optionally, the PS-TOAs for the I2R NDPs received from other ISTAs participating in the passive TB ranging (i.e. polling, sounding, and reporting triplet) identified by the Sounding Dialog Token Number– labeled with their respective AID12/RSID12s.

The ISTA Passive TB Ranging Measurement Report frame shall include an entry for the ISTA's I2R NDP TOD.

The ISTA shall set the More subfield in the More & N Timestamp Measurements Report field in the ISTA Passive TB Ranging Measurement Report element contained in the ISTA Passive TB Ranging Measurement Report frame to 1 if it has more timestamps ready to report but does not have space in its allocated resources by the RSTA for ISTA Passive TB Ranging Measurement Report frame. Else the ISTA shall set the More subfield to 0.

The RSTA shall send the Primary and Secondary RSTA Broadcast Passive TB Ranging Measurement Report frames, the Primary a SIFS time after receiving the ISTA Passive TB Ranging Measurement Report frames from the ISTA and the Secondary a SIFS following the Primary; see Figure [11-37x](#F11o37x) (Passive TB ranging measurement reporting phase).

The Primary RSTA Broadcast Passive TB Ranging Measurement Report frame shall contain the following:

* Passive TB Ranging LCI Table Counter
* Passive TB Ranging LCI Table Countdown Info
* RSTA Passive TB Ranging Measurement Report
* Passive TB Ranging LCI Table (optionally present)

Each time an RSTA transmits a Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, it shall set the Passive TB Ranging LCI Table Counter value such as to refer to the latest version of the Passive TB Ranging LCI Table element transmitted by the RSTA.

If a Passive TB Ranging LCI Table element is included in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, and this element has different content as compared to the last transmitted Passive TB Ranging LCI Table element, then Passive TB Ranging LCI Table Counter shall be incremented by 1 (modulo 256) from the value associated with the previous Passive TB Ranging LCI Table element content. (The first time the RSTA transmits a Passive TB Ranging LCI Table element the value shall be set to 0). This new value of the Passive TB Ranging LCI Table Counter is now associated with this new version of the Passive TB Ranging LCI Table element.

If a Passive TB Ranging LCI Table element is included in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, and this element has the same content as the last transmitted Passive TB Ranging LCI Table element, then Passive TB Ranging LCI Table Counter value shall be the value associated with this last version of the Passive TB Ranging LCI Table element transmitted by the RSTA.

If a Passive TB Ranging LCI Table element is not included in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, then the Passive TB Ranging LCI Table Counter value shall be the value associated with the last version of the Passive TB Ranging LCI Table element transmitted by the RSTA.

When the Passive TB Ranging LCI Table is present in the Primary Broadcast Passive TB Ranging Measurement Report frame, the RSTA LCI Report field of the Passive TB Ranging LCI Table Report element shall contain the Antenna Placement and Calibration subelement if the RSTA has dot11PassiveTBRangingAODImplemented equal to true, and shall not contain the Antenna Placement and Calibration subelement if the RSTA has dot11PassiveTBRangingAODImplemented equal to false.

When the Passive TB Ranging LCI Table is present in the Primary Broadcast Passive TB Ranging Measurement Report frame, the corresponding entree of the ISTA LCI Reports Entries field of the Passive TB Ranging LCI Table Report element shall contain the Antenna Placement and Calibration subelement if the ISTA has dot11PassiveTBRangingAoDImplemented equal to true, and shall not contain the Antenna Placement and Calibration subelement if the ISTA has dot11PassiveTBRangingAODImplemented equal to false.

The Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame shall contain the following:

* ISTA Passive TB Ranging Measurement Reports

See Subclause [9.6.7.52](#H09o6o7o52) (Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame format).

When phase shift feedback is negotiated between an ISTA and an RSTA in Passive TB ranging, the protocol for the measurement reporting phase differs from Passive TB ranging with TOA feedback on the following points:

* The RSTA shall report its measured PSTOA in the R2I LMR frame.
* The ISTA shall report its measured PSTOA(s), in addition to its measured TOA(s), in the ISTA Passive TB Ranging Measurement Report frame.
  + The PSTOAs are indicated as phase shift TOA timestamps by setting the Measurement Report field of the ISTA Passive TB Ranging Measurement Report element, see [9.4.2.304](#H09o4o2o304) (ISTA Passive TB Ranging Measurement Report element), to the value 10 (PSTOA).
* In the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, the RSTA shall send a broadcast frame containing its measured PSTOA, in addition to its measured TOA, for the I2R NDPs it has received from the ISTA.
* In the Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame the RSTA shall rebroadcast the timestamps the ISTA has reported to the RSTA. As the ISTA has negotiated phase shift feedback, these would contain PSTOAs in addition to TOAs.

When phase shift feedback is negotiated in Passive TB ranging, the reporting by both the RSTA and the ISTA of phase shift TOAs, the TOD, and CFO shall be immediate feedback. The reported TOAs may be immediate or delayed feedback. When the TOA feedback is delayed, the dialog token shall refer to the previous measurement instance for the RSTA-ISTA pair.

The TODs and PSTOAs measured by the RSTA shall be broadcast in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame in the reporting phase following the measurement exchange in which they were measured.

The CFO, TOD, and PSTOAs reported by the ISTA shall be rebroadcasted in the Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame in the reporting phase following the measurement exchange in which they were measured.

***Insert the following new clause:***

**11.21.6.4.9 Passive TB ranging differential time-of-flight calculations using phase shift TOA timestamps**

In Figure [11-37y](#F11o37y) (Example of passive TB ranging measurement exchanges with PSTOA measurements), passive TB ranging measurement exchanges and their reception by a passive station, a PSTA, are depicted for the case when the RSTA and the ISTA are measuring and reporting phase shift TOAs, PSTOAs; see Annex [AD.1](#AnnexADo1) for how the phase shift TOAs are calculated.

The RSTA measures the PSTOA tp2 and the ISTA measures the PSTOA tp4, in addition to measuring their TODs, t3 and t1 respectively. The ISTA also measures its CFO with respect to the RSTA. The ISTA reports its CFO and timestamps to the RSTA and the RSTA broadcasts these as well as its own timestamps to the PSTA.

The ISTA also measures and reports the TOA timestamps for the ranging NDPs it receives and the RSTA also measures and broadcasts the TOAs of the ranging NDPs it receives, as well as the ISTAs reported TOAs, though these timestamps are not used in the calculations described here.

****

**Figure 11-37y—Example of passive TB ranging measurement exchanges with PSTOA measurements.**

The differential time of flight from the PSTA to the RSTA and the ISTA (DToF\_PRI) is defined by Equation [(11-6i)](#E11o6i):

DToF\_PRI = ToF\_PR – ToF\_PI, (11-6i)

Where, ToF\_PR is the time of flight between the PSTA and the RSTA, and the ToF\_PI is the time of flight between the PSTA and the ISTA.

The differential time of flight (DToF\_PRI) can then be computed as as per Equation [(11-6j)](#E11o6j):

DToF\_PRI = t6 – t5 – 0.5 × t3’ + 0.5 × tp2’ – 0.5 × tp4’ + 0.5 × t1’.  (11-6j)

The timestamp t1’ is the time at which the I2R NDP was transmitted from the ISTA and the timestamp tp4’ is the PSTOA measurement for the time at which the R2I NDP was received by the ISTA, converted from the ISTA’s time basis to the PSTA’s time basis.

The timestamp tp2’ is the PSTOA measurement for the time at which the I2R NDP was received by the RSTA and t3’ is the time at which the R2I NDP was transmitted from the RSTA, converted from the RSTA’s time basis to the PSTA’s time basis.

At the PSTA, the mechanism by which t1’ and tp4’ is derived from t1, tp4, the ISTA’s reported CFO, and the PSTA’s CFO measured with respect to the RSTA is implementation dependent.

At the PSTA, the mechanism by which t2’ and tp3’ is derived from t2, tp3, and the PSTA’s CFO measured with respect to the RSTA is implementation dependent.

**3.2 Definitions specific to IEEE 802.11**

***TGbk editor: Please update subclause 3.2 as follows (track changes enabled):***

**Null-SAC-LTF** : A LTF present in an initiating STA (ISTA) to a responding STA (RSTA) null data PPDU (NDP), or RSTA to ISTA NDP in the Ranging frame exchange, resulting from a mismatch of sequence authentication code (SAC) subfield in the STA Info field of a Ranging NDP Announcement frame, or the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame, with either the value of the Validation SAC subfield in the Secure LTF Parameters element in the last transmitted FTM frame, or the last transmitted Location Measurement Report frame to the ISTA, or is equal to 0 . The TXVECTOR LTF\_KEY and LTF\_IV parameter corresponding to this LTF are set to generate any secure LTF or null.

***TGbk editor: Please delete “HE-“ from Figure 9-788eu (*Secure HE-LTF Parameters element format*) as follows and make corresponding update throughput the 11az text where the Secure LTF Parameters element or the Secure LTF Counter field in the element is referred to (track changes enabled):***

**9.4.2.299 Secure LTF Parameters element**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 B7 | B8 B15 | B16 B23 | B24 B71 | B72 B87 | B88 B103 | B104 B111 |
|  | Element ID | Length | Element ID Extension | Secure LTF Counter | Validation SAC | Measurement SAC | Measurement Result LTF Offset |
| Octets: | 1 | 1 | 1 | 6 | 2 | 2 | 1 |

**Figure 9-788eu—Secure LTF Parameters element format**

**Straw Poll: Do you support to incorporate the proposed draft text in this document 11-23/0698r2 to the TGbk Draft?**

**Result: Yes/No/Abstain**